简译版

探寻“威胁猎杀”的真正含义

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Hunting for the True Meaning of Threat Hunting at RSAC 2019		
原文作者	Jake Munroe	**原文发布日期**	2019 年 3 月 21 日
作者简介	Jake Munroe 是 IBM Security i2 团队的产品营销经理。 https://securityintelligence.com/author/jake-munroe/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/hunting-for-the-true-meaning-of-threat-hunting-at-rsac-2019/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

探寻“威胁猎杀”的真正含义

Jake Munroe

2019 年 3 月 21 日

今年，我第一次参加 RSA 大会，收获满满回到了波士顿。大会期间，我大部分时间花在 IBM Security 公司的“威胁猎杀”（Threat Hunting）展位上。在那里，我向与会者介绍如何使用军方和情报界的方法和工具来对抗企业的网络威胁。当我不在展位时，我就开始自己的探寻之旅——探寻“威胁猎杀”的真正含义。

不要相信炒作：关于“威胁猎杀”的三个常见误解

乍一看，我的探寻之旅似乎很有收获——我看到许多供应商的展位上都有“威胁猎杀”一词。为了获得更多的信息，我与展位工作人员讨论他们的威胁猎杀解决方案，拿回一堆宣传手册，然后继续探寻。

在与多家供应商的展位工作人员沟通并深入分析其宣传手册之后，我很遗憾地发现，“威胁猎杀”一词正在成为流行语。

老实说，威胁猎杀听起来很酷，吸引着人们去了解更多信息。但是，需要注意的是，威胁猎杀其实是一种网络调查方法，这种方法早在营销人员将其作为噱头之前就已经存在了。

以下是我在 RSA 大会上发现的关于威胁猎杀的三个误解。

1. 威胁猎杀应该是完全自动化的

自动化很棒，我也喜欢将生活中的某些部分自动化，这样能够节省时间，使生活更轻松。但是，有些事情不能实现完全的自动化（或者说不应该实现完全的自动化），至少现在还不能。威胁猎杀就是其中之一。

虽然各种威胁猎杀工具都可以使用自动化技术，但威胁猎杀仍然是一个倾向于手动的、以“人”为主导的过程，以主动寻找网络中的未知威胁（这些威胁能够规避基于规则的检测解决方案）。威胁猎杀方法源自反恐界，并应用于网络安全领域。反恐分析没有实现完全的自动化是有原因的，而这个原因同样适用于网络安全领域。

2. 将威胁猎杀和 EDR 混为一谈

这是最常见的误解。事情是这样的：我进入一个展位，向工作人员询问威胁猎杀解决方案，发现他们销售的其实是端点检测和响应（EDR）解决方案。

EDR 是威胁猎杀的关键部分，但它们并不是“威胁猎手”（threat hunter）使用的唯一工具。如果威胁猎杀像使用 EDR 解决方案来检测威胁一样简单，我们就会有更高的猎杀成功率了。事实上，EDR 解决方案需要与其他工具结合使用，例如威胁情报、开源情报（OSINT）和网络数据，并将它们集成在一个通用平台中，以便实现数据的可视化，识别异常情况。

3. 将威胁猎杀想的过于复杂

很多供应商将威胁猎杀想的过于复杂了。它不是一个工具、不是完全自动化的，但也不是非常复杂的过程。它需要多种工具和大量数据，高度依赖训练有素的分析师（他们知道寻找什么）。此外，就像反恐和执法调查一样，威胁猎杀也是一个调查过程。威胁猎杀涉及各种调查技术，因此威胁猎手应关注来自国家安全和执法部门的可靠工具。

威胁猎杀究竟是什么？

不要误解我的意思——我很高兴看到威胁猎杀的发展，以及供应商不断提出创新的解决方案来定义威胁猎杀。作为一名前分析师，我将威胁猎杀定义为深入的、以“人”为主导的调查过程，旨在发现企业的威胁。我的定义可能与大多数定义有所不同——大多数定义都认为威胁猎杀是一种完全主动的方法。虽然我认同主动性的重要性，但由于预算、培训和时间等限制，很少有企业能够采取主动的方法来进行威胁猎杀。

虽然不够理想，但有一种方法可以响应性地进行猎杀，这对于中小型企业来说更为现实。例如，企业可以进行更深入的网络调查，以获取有关网络事件或告警的背景信息。有人认为这只是事件响应，而不是威胁猎杀。但是，当分析师采用全源情报方法（包括外部数据源[威胁情报和社交媒体等]和内部数据源）进行调查时，它就是威胁猎杀了。这种方法可以显示与事件相关的人、事、地点、时间和方式，并告知领导层如何采取最佳行动。背景信息也可用于训练基于规则的系统，并为将来的调查分析建立基准。

威胁猎杀的定义不断演变

网络威胁猎杀工具多种多样，但是最先进的工具可以将所有内部和外部数据集中到一个

平台上，来响应性地、主动地调查威胁。通过融合内部安全信息和事件管理（SIEM）数据、内部记录、访问日志以及更多外部数据源，威胁猎手可以识别数据中的趋势和异常，并将其转化为可操作的情报，以主动响应网络中的威胁。

在 RSA 大会之后，威胁猎杀将继续受到关注。供应商将开发出更先进的解决方案，帮助企业更有效地捕获威胁。将来，威胁猎杀的定义还会继续演变——我很期待看到这一点，前提是威胁猎杀的基础是稳健的。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*